BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-230

4 AUGUST 2004

Communications and Information

INFORMATION ASSURANCE ASSESSMENT AND ASSISTANCE PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: HQ AFCA/WFPL (MSgt Eric J. Wolfe)

Certified by: HQ USAF/XICI (Lt Col Tracy A. Phillips)

Supersedes AFI 33-230, 28 September 2000

Pages: 17

Distribution: F

This instruction implements National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4005, *Safeguarding Communications Security (COMSEC) Facilities and Materials*, and Air Force Policy Directive (AFPD) 33-2, *Information Protection* (will become *Information Assurance*). This instruction establishes the Information Assurance Assessment and Assistance Program (IAAP) and applies to all Air Force units and personnel, including civilians under contract by the Department of Defense, who use information systems. This publication applies to the Air National Guard (ANG). Direct technical changes or questions pertaining to this instruction to Headquarters Air Force Communications Agency (HQ AFCA/WFP), 203 W Losey St, Room 2200, Scott AFB IL 62225-5222. Refer recommended changes and conflicts between this and other publications on AF Form 847, **Recommendation for Change of Publication,** through channels to HQ AFCA/ITXD, 203 W. Losey St. Room 1100, Scott AFB IL 62225-5222. Send supplements to this publication to HQ AFCA/WFP for review, coordination, and approval prior to publication. Public Law 104-13, *Paperwork Reduction Act of 1995*, and Air Force Instruction (AFI) 33-360, Volume 2, *Content Management Program—Information Management Tool (CMP-IMT)*, affect this publication. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records,* and disposed of in accordance with Air Force Web-RIMS Records Disposition Schedule (RDS) located at **https://webrims.amc.af.mil/rds/index.cfm**. See **Attachment 1** for a glossary of references and supporting information.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

This revision updates terminology and office symbols throughout the entire document. It adds HQ USAF responsibilities and updates the order of the activities under responsibilities. Identifies grade requirements for major command (MAJCOM) team chief. Provides the criteria for events that drive an earlier assessment of the wing by the MAJCOM. Creates an executive summary and a detailed report. Adds tables for

processing and routing reports, initial and follow-up replies, annual summary reports, and usage of each section of the AF IMT 4160, **Information Assurance Assessment and Assistance Program (IAAP) Criteria**. It also provides a table to determine the rating of the Information Assurance Assessment and Assistance Program (IAAP). Added are examples of the executive summary report, the detailed report, an initial reply, a follow-up reply, and an example of the annual summary report.

1. Purpose. The IAAP's purpose is to "find and fix" wing-level information assurance (IA) problems, essentially staff assistance, therefore, it is not a function of, or to be replaced by, Inspector General (IG) or Audit Agency activities. The IAAP accomplishes "staff assistance" by reviewing and assessing processes, identifying problems, providing assistance to help resolve the problems, and recommending solutions. The IAAP team provides technical and training assistance in all IA areas. The IAAP also includes the auditing of all communications security (COMSEC) materials and records mandated by the National Security Agency and defined in NSTISSI 4005. The IAAP consists of two parts: assessment and assistance. Areas to be assessed are to be found on AF IMT 4160, **Information Assurance Assessment and Assistance Program (IAAP) Criteria**, and can be located at **https://private.afca.af.mil/ip**.

NOTE: All references to wing-level IA programs in this AFI represent similar levels such as bases and geographically separated units.

1.1. **Assessments.** Using AF IMT 4160 IAAP teams will assess:

1.1.1. Effectiveness of the wing IA program to include COMSEC (AFI 33-201, *Communications Security (COMSEC)*), network and computer security (AFI 33-202, *Network and Computer Security*), emission security (EMSEC) (AFI 33-203, *Emission Security*), IA awareness (AFI 33-204, *Information Awareness (IA) Awareness Program*), information protection operations (AFI 33-115, Volume 1, *Network Management*), network user licensing and the certification of network user licensing (AFI 33-115,Volume 2, *Licensing Network Users and Certifying Network Professionals*), password management (AFMAN 33-223, *Identification and Authentication),* and other areas of interest covered on AF IMT 4160.

1.1.2. Security posture of wing information systems and the information contained therein.

1.1.3. Security of computer systems associated with information-dependent systems (i.e., telephone switches, air traffic, base security alarm, sensor, space systems, etc.).

1.1.4. Security, availability, and reliability of systems supporting the base information infrastructure.

1.1.5. Quality of the wing COMSEC operations and a 100 percent audit of all COMSEC keying material.

NOTE: This applies to all COMSEC accounts whose numbers begin with a 6 or 7, including contractors having Air Force accounts.

1.1.6. Quality of security training provided to individuals using information systems, systems administrators, workgroup managers, personnel responsible for COMSEC material, personnel assigned to the network control center (NCC), and wing IA personnel.

1.1.7. Actions taken based on Air Force and major command (MAJCOM) Time Compliance Network Order

1.2. **Assistance.** IAAP teams are not required to "fix" all identified problems but to assist users, systems administrators, network managers, designated approving authorities, unit security personnel, NCC, and wing IA personnel in the resolution of identified problems. This includes, but is not limited to, technical, administrative, and training assistance. Additionally, the IAAP team will refer assessed organizations to the appropriate organizations which may provide follow-on assistance.

2. Responsibilities:

2.1. **Headquarters United States Air Force, Deputy Chief of Staff/Warfighting Integration, Information Assurance Division (HQ USAF/XICI):**

2.1.1. Serves as the Air Staff office of primary responsibility (OPR) for the IAAP.

2.1.2. Directs changes to policy, procedures and criteria based on problems identified in the annual summary of IAAP reports.

2.1.3. Provides applicable Air Staff offices a copy of the IAAP Annual Summary Report.

2.2. **Headquarters Air Force Communications Agency (HQ AFCA):**

2.2.1. Develops, coordinates with HQ USAF/XICI, publishes, and maintains the IAAP Checklist (AF IMT 4160) and works with HQ USAF/XICI to establish critical items.

2.2.2. Periodically accompanies MAJCOMs, and, if requested, assists them during MAJCOM IAAP visits. Keeps visits to the minimum necessary to maintain currency with wing IA and NCC functions and responsibilities.

2.2.3. Tracks and monitors MAJCOM's IAAP schedule.

2.2.4. Reviews IAAP reports to identify overall weaknesses in the Air Force IA program by recommending changes to policy and procedures.

2.2.5. Reviews IAAP reports and has the final authority to downgrade IAAP report ratings when it is clear that incidents or deviations are involved.

2.2.6. Provides HQ USAF/XICI an annual summary of the results of MAJCOM conducted IAAPs.

2.2.7. Performs IAAPs for organizations where HQ AFCA is identified as monitoring headquarters for the supporting COMSEC account, as listed in AFKAG-28, *COMSEC Account Directory*.

2.3. **Air Force Information Warfare Center (AFIWC):**

2.3.1. Provides technical support to MAJCOM IAAPs according to AFPD 33-2, AFI 33-207, *Computer Security Assistance Program,* and this instruction.

2.3.2. Provides inputs and comments to the MAJCOMs during the assessment for the MAJCOM's IAAP detailed report.

2.4. **MAJCOMs:**

2.4.1. Implement and manage a command IAAP.

2.4.1.1. Coordinate the scheduling of the IAAP visit with the unit, agencies within the MAJCOM (i.e., IG, gatekeeper, etc.), and other agencies outside the MAJCOM (i.e., Scope Net, auditors, etc.) to avoid or minimize scheduling conflicts.

2.4.1.2. Send IAAP schedules to HQ AFCA/WFP for tracking and monitoring.

2.4.1.3. Deconflict scheduling between the IAAP visit and other agencies; the MAJCOM IA office will determine the appropriateness of performing an IAAP at that time. As a minimum, perform the COMSEC assessment and audit as near to the 2-year requirement as possible. Provide units with as much notice as possible. No-notice IAAP assessments are not authorized.

2.4.2. Establish IAAP teams consisting of personnel with experience in base information infrastructures, information systems, and IA. Personnel performing assessments must have extensive on-the-job experience in the area they are assessing and must understand the "staff assistance" nature of IAAPs.

2.4.2.1. The minimum grade required for the IAAP team chief is an officer, a senior noncommissioned officer (NCO), or GS-11 or above. IAAP team members may include contractor personnel.

2.4.2.2. The lead individual assessing and auditing COMSEC operations must be the same rank required as a COMSEC manager (MSgt, GS-9 civilian, or above).

2.4.3. Conduct assessments of wing IA programs using AF IMT 4160 every 2 years or sooner based on the following specific events or situations:

2.4.3.1. Within 6 months of a change of COMSEC manager, if requested. Under these circumstances, the IAAP may be limited to an assessment of the COMSEC function.

2.4.3.2. Correspondence that is consistently late or nonexistent.

2.4.3.3. Influx or increase in incidents, vulnerabilities, or other disturbing activities, which might indicate cause for concern.

2.4.3.4. Upon request from the wing or unit commander.

2.4.3.5. Overseas units with tour of duty less than 18 months.

2.4.3.6. Within 60 days of activation or deactivation of a contractor COMSEC account.

2.4.4. In coordination with the ANG, conduct assessments of gained ANG units.

2.4.5. Use technical support from the AFIWC or the MAJCOM Network Operations and Security Center (NOSC). Request support for AFIWC at least 60 days prior to scheduled MAJCOM IAAP visits to coordinate schedules.

2.4.6. After the IAAP assessment, outbrief the wing commander. Include the wing IA office, unit commanders who have critical deficiencies identified (e.g., a NO is answered for a critical question), the unit commander of the IA office, and the wing IA manager. Describe the posture of the wing IA program and the security of the base information infrastructure by summarizing and identifying critical deficiencies. ***NOTE:*** For contractor COMSEC accounts, also outbrief the contractor's Facility Security Officer (FSO).

2.4.7. Provide an executive summary and a detailed report according to **Table 1.**

2.4.8. Provide an annual summary of the MAJCOM IAAPs according to paragraph **3.7.**, **Table 4.**, and **Attachment 6**.

2.5. **Wings:**

2.5.1. Perform semiannual self-assessments of wing COMSEC operations and annual IA self-assessments on behalf of the wing commander**,** using the AF IMT 4160.

2.5.1.1. Assess all host and tenant units (includes ANG and Air Force Reserve Command (AFRC) units) who use any IA services of the wing (e.g., use the base information network, telephone service, COMSEC material, etc.).

2.5.1.2. The Wing IA office will support ANG and AFRC units who are tenants on their bases. If the ANG or AFRC unit has an established COMSEC account, the wing IA is responsible for all other IA support except for COMSEC.

2.5.2. Provide technical support such as on-line surveys, site traffic, and network mapping information to visiting MAJCOM IAAP teams.

2.5.3. Outbrief the unit commander on the organization's IA posture by summarizing any identified critical deficiencies and laudatory observations. Briefing the wing commander is not required unless recurring critical items have been identified.

2.5.4. Provide an executive summary and a detailed report according to **Table 1.**

2.5.5. Provide an annual summary of the wing IAAPs according to paragraph **3.7.**, **Table 4.**, and **Attachment 6**.

3. Reports. IAAP reports consist of executive summaries, detailed reports, initial replies, follow-up replies, and annual summaries.

3.1. **Report Preparation.** MAJCOMs and wings document the results of all IAAPs in narrative format as executive summaries and detailed reports. Properly classify and mark IAAP reports according to AFMAN 33-272 (S), *Classification of Communications Security, TEMPEST, and C4 Systems Security Research and Development Information* (U) (will become Information Assurance Classification Guide). This report is exempt from report control symbol reporting according to AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections.*

3.1.1. The IAAP executive summary report will reflect the status of the IA posture of the wing: all critical deficiencies found; impact if the deficiencies are not corrected; assistance provided; and recommendations (see **Attachment 2**).

3.1.2. The IAAP detailed reports will include: deficiencies and impact if not corrected; significant problems; those problems resolved on-site (found and fixed); those that still require resolution with recommendations; and any additional assistance provided by the IAAP team (see **Attachment 3**).

NOTE: Significant problems are those which have not been identified as critical items, but if not corrected could lead to more serious problems.

3.2. **Rating Criteria.** The IAAP will be rated satisfactory or unsatisfactory. Critical questions are identified on the AF IMT 4160 with a "#" sign before the number. Use **Table 1.** to determine the ratings for each section and the overall rating. Take into consideration the impact of discrepancies identified when determining the rating. Rate each section individually, and provide a final overall rating for the entire wing IA program.

3.2.1. Unsatisfactory ratings. At a minimum, reassess those areas that were rated unsatisfactory.

3.2.2. Wings: Reassess units receiving unsatisfactory assessments within 90 days.

3.2.3. MAJCOM: Reassess bases receiving unsatisfactory assessments no earlier than 90 days but within 180 days.

Table 1. Determine Rating for IAAP.

On section:	**of the AF IMT 4160, if the number of critical questions that are not favorable equals**	**and the number of noncritical questions answered favorable equals**	**then the overall rating is:**
One	50% or greater	70% or greater	Satisfactory
Two		Less than 70%	Unsatisfactory
Three	Less than 50%	70% or greater	
		Less than 70%	
Four	None	70% or greater	Satisfactory
		Less than 70%	Unsatisfactory
	One or more	70% or greater	
		Less than 70%	

NOTES:

1. For MAJCOM and wing IAAPs: Use sections one, two, and three.
2. Use section four as a self-assessment by the MAJCOM/field operating agency (FOA)/ direct reporting unit (DRU) or by an outside agency assessing the MAJCOM.
3. Rating is based from the questions in the AF IMT 4160 checklist only. This is to standardize the overall IAAP; rating will be based on the question on the AF 4160 checklist.

3.3. **Reports Processing and Routing.** Process and route reports according to **Table 2.** When a MAJCOM other than the assessed activity's headquarters performs a review, the assessing activity processes the report and forwards it to the assessed activity's MAJCOM IA office for processing.

Table 2. Processing and Routing Reports.

Type of Report	Process report within:	Route reports	
		Action to:	Info to:
MAJCOM Executive Summary	20 working days	Wing Commander	Wing IA Unit Commander and Wing IA Office
MAJCOM Detailed Report	10 working days	Wing IA Unit Commander	Commander of Assessed Units (Note 1), Wing IA Office, and HQ AFCA/WFP
Wing Executive Summary	20 working days	Wing Commander (Note 2)	Commander of Assessed Units
Wing Detailed Report	10 working days	Commander of Assessed Unit	Assessed Unit

NOTES:

1. If any critical items are identified for a unit, then address a copy of the report to the commander of assessed unit.
2. This report is only needed if critical items are identified.

3.4. **Report Responses.**

3.4.1. Assessed activities must respond to all deficiencies identified in reports. Replies must address the specific actions taken to correct and eliminate the basic root cause of the deficiencies and provide enough detail to permit effective evaluation (See **Attachment 4** and **Attachment 5**).

3.4.2. Endorsements (**Table 3.**) must provide a concurrence or non-concurrence with corrective actions taken and definitive plans to resolve uncorrected deficiencies.

3.5. **Initial Replies.** Prepare the initial reply in the format provided in **Attachment 4**. Process initial reports according to **Table 3.**

3.6. **Follow-up Replies.** Prepare the follow-up reply in the format provided in **Attachment 5**. Process follow-up reports according to **Table 3.**

Table 3. Processing and Routing Initial and Follow-up Replies.

Type of report	Initial follow-up due	Then, follow-up reporting is due in:	Reports are endorsed by:	Authority for closing report:
MAJCOM	10 working days	60 days (Note 1)	Unit Commander(s) (Note 2)	MAJCOM IA office (Note 3)
Wing		30 days (Note 1)	Unit Commander	Wing IA office (Note 3)

NOTES:

1. Follow-ups are due on all open items until closed by the office listed in the last column to the far right.
2. Unit commanders of all units identified as having deficiencies will endorse the reports until the item is corrected for that unit.
3. The authority determines the adequacy of responses and is responsible for closing the critical deficiencies and the report.

3.7. **Annual Summary Reports.** Prepare and route annual summary reports according to **Table 4.** Prepare the summary report in the format provided in **Attachment 6**. At a minimum, the summary will identify all critical deficiencies identified, impacts and recommended solutions, including recommended changes to policy and procedures. The MAJCOM summary report will identify bases that are overdue for assessment and reasons for noncompliance. The overdue bases will be matched up with the HQ AFCA database and included in the final report sent to HQ USAF/XICI. The report will be provided to the addresses by the due date listed in **Table 4.** The annual summary report from AFCA will also be incorporated into the annual IA metric report reported according to AFI 33-205, *Information Protection Metrics and Measurements Program*.

Table 4. Processing and Routing Annual Summary Reports.

Report By:	Due Date:	Route reports	
		Action to:	Info to:
Wing	15 Jan	Wing Commander	MAJCOM IA Office
MAJCOM	1 Feb	MAJCOM/SC	HQ AFCA/WFP
AFCA	15 Feb	HQ USAF/XICI	MAJCOM/SC (or equivalent)

4. AF IMT 4160, Information Assurance Assessment and Assistance Program (IAAP) Criteria. Use the AF IMT 4160 sections as prescribed in **Table 5.**

Table 5. Usage of Each Section of the AF IMT 4160.

Section:	Applies to:	Used for:	Usage by Wings:	Usage by MAJCOM:
One	Units	Self-assessments and Wing IAAPs	Semiannually for CRO questions, annually for all other questions	During MAJCOM IAAP
Two	Wing IA Office	Self-assessments and MAJCOMs IAAPs	Semiannually for COMSEC questions, annually for all other questions	
Three	Host Wing Units		Annually	
Four	MAJCOMs/ FOAs/DRUs	Self-assessments and by other outside agencies	N/A	As needed

5. Information Collections, Records, and Forms or Information Management Tools (IMT) .

5.1. Information Collections. Annual Multi-Disciplinary Review Board RCS SAF-PAS(A) 0203 (see paragraph **3.1.**).

5.2. Records. Records pertaining to executive summary report, the detailed report, an initial reply, a follow-up reply, and the annual summary report are created by this publication (paragraph **3.**). Retain and dispose of these records according to Air Force Web-RIMS RDS, Table 37-18, Rule 17, located at **https://webrims.amc.af.mil/rds/index.cfm**.

5.3. Forms or IMTs (Adopted and Prescribed).

5.3.1. Adopted Forms or IMTs: AF Form 847, **Recommendation for Change of Publications**.

5.3.2. Prescribed Forms or IMTs: AF IMT 4160, **Information Assurance Assessment and Assistance Program**.

WILLIAM T. HOBBINS, Lt General, USAF
DCS, Warfighting Integration

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Public Law 104-13, *Paperwork Reduction Act of 1995*

NSTISSI No. 4005, *Safeguarding Communications Security (COMSEC) Facilities and Materials*

AFPD 33-2, *Information Protection* (will become *Information Assurance*)

AFI 33-115, Volume 1, *Network Management*

AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals*

AFI 33-201, *Communications Security (COMSEC)*

AFI 33-202, *Network and Computer Security*

AFI 33-203, *Emission Security*

AFI 33-204, *Information Assurance (IA) Awareness Program*

AFI 33-205, *Information Protection Metrics and Measurements Program*

AFI 33-207, *Computer Security Assistance Program*

AFMAN 33-223, *Identification and Authentication*

AFMAN 33-272 (S), *Classification of Communications Security, TEMPEST, and C4 Systems Security Research and Development Information (U) (*will be *Information Assurance Classification Guide)*

AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*

AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*

AFMAN 37-123, *Management of Records*

AFKAG-28, *COMSEC Account Directory*

Air Force Web-RIMS Records Disposition Schedule (RDS)

Abbreviations and Acronyms

AFCA—Air Force Communications Agency

AFI—Air Force Instruction

AFIWC—Air Force Information Warfare Center

AFMAN—Air Force Manual

AFSSI—Air Force Special Security Instruction

AFPD—Air Force Policy Directive

AFRC—Air Force Reserve Command

ANG—Air National Guard

COMSEC—Communications Security

CRO—COMSEC Responsible Officer

DRU—Direct Reporting Unit

EMSEC—Emission Security

FOA—Field Operating Agency

FSO—Facility Security Officer

IA—Information Assurance

IG—Inspector General

IAAP—Information Assurance Assessment and Assistance Program

MAJCOM—Major Command

NCC—Network Control Center

NCO—Non-Commissioned Officer

NOSC—Network Operations and Security Center

NSTISSI—National Security Telecommunications and Information Systems Security Instruction

OPR—Office of Primary Responsibility

RDS—Records Disposition Schedule

USAF—United States Air Force

Terms

AFKAG—A short title used on Air Force general operational publications. Some of these publications are handled through COMSEC Material Control System (CMCS) channels.

Information Assurance (IA)—Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Assurance Assessment and Assistance Program (IAAP)—A function established to assess the effectiveness of wing IA programs and to provide assistance, when necessary.

Information Systems—Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.

Attachment 2

EXAMPLE OF EXECUTIVE SUMMARY REPORT OF INFORMATION ASSURANCE ASSESSMENTS AND ASSISTANCE PROGRAM VISITS

MEMORANDUM FOR (Wing Commander)

FROM: MAJCOM/SC (or equivalent)

SUBJECT: Executive Summary Report of IAAP Visit

Section I – General

1. (Names of IAAP team members including any supporting teams such as AFIWC, or auditors, etc.) conducted the IAAP of the (list wing and base), from (inclusive dates of the assessment). The assessment provides valuable insight into the information assurance posture of (wing/site name). The previous assessment and assistance visit was conducted (date). The authority for this assessment is AFI 33-230, *Information Assurance Assessment and Assistance Program*.

2. (Summarize all items including impact if not corrected, assistance provided, and recommendations. Also, identify any other items that have an impact on the security posture of the wing/site.)

3. A detailed report has been sent to the Wing IA office and follow-up reporting is required on all items.

Signature Block

Attachment 3

EXAMPLE OF DETAILED REPORT OF INFORMATION ASSURANCE ASSESSMENTS AND ASSISTANCE PROGRAM VISITS

MEMORANDUM FOR (Unit Commander of Wing IA Office)

FROM: MAJCOM

SUBJECT: Detailed Report of Information Assurance Assessment and Assistance Program (IAAP) Visit

Section I – General

1. (Names of IAAP team members including any supporting teams such as AFIWC, or auditors, etc.) conducted the IAAP of the (list wing and base), from (inclusive dates of the assessment). The assessment provides valuable insight into the information assurance posture of (wing/site name). The previous assessment and assistance visit was conducted (date). The authority for this assessment is AFI 33-230, *Information Assurance Assessment and Assistance Program*.

2. Personnel contacted: (List name and rank of key personnel contacted including the unit and position held.)

Section II - Findings/Impact/Recommendations

3. Deficiencies identified using AF IMT 4160, **Information Assurance Assessment and Assistance Program (IAAP) Criteria**.

Item 1. (List section and question number)

a. Finding: (Identify findings, include if critical deficiencies, significant problem or if problem was corrected on the spot.)

b. Ref: (Provide specific paragraph reference in an AFI, AFSSI, other specialized publication, or policy message.)

c. Impact: (Critical items must identify impact if not corrected.)

d. Recommendation: (Provide recommended solution to correct the problem.)

Item 2 (Report all items for each finding.)

a. Finding:

b. Ref:

c. Impact:

d. Recommendation:

Section III - Other Comments:

4. Other Deficiencies. (This area is for deficiencies found that are not listed on the AF IMT 4160, however, a publication [AFI, AFSSI, AFKAG, etc.] or a policy message exists mandating the deficiency.)

a. Finding:

b. Ref:

c. Impact:

d. Recommendation:

5. Summary of Assistance Provided. (Identify those areas where assistance was provided ["found and fixed"] by the IAAP team members.)

6. Laudatory comments. (Use this area for any person, product, best practice, etc., which is worth mentioning.)

7. Request you endorse this report through IA channels within 10 working days of receipt. If you are unable to correct critical deficiencies in the 10 days, then provide the status of the corrective actions under way and include the estimated completion date.

Signature Block

Attachment 4

EXAMPLE OF INITIAL REPLY TO INFORMATION ASSURANCE ASSESSMENT AND ASSISTANCE PROGRAM (IAAP) VISIT

MEMORANDUM FOR (MAJCOM IA Office)

FROM: (Wing IA Office)

SUBJECT: Initial Reply to Information Assurance Assessment and Assistance Program (IAAP) Visit, (include dates)

Section I - General

1. This is our initial reply to the IAAP conducted by (MAJCOM IA Office) from (dates of assessment). The following is the status of all deficiencies identified during the IAAP visit.

Section II – Findings/Impact/Recommendations

Item 1. (List section and question number)

a. Comments: (State the actions taken to correct the deficiency.)

b. Status: (State if the action is open or if it completed and is recommended to be closed.) (If the item is still open then:) Estimated completion date is (provide a date).

2. (Additional comments.)

3. (List POC, office symbol, phone numbers, and e-mail address.)

Signature Block

1st Ind, (Unit commander)

MEMORANDUM FOR (MAJCOM IA Office)

(Provide a concurrence or nonconcurrence with corrective actions taken and definitive plans to resolve uncorrected deficiencies.)

Signature Block

Attachment 5

EXAMPLE OF FOLLOW-UP REPLY TO IAAP VISIT

MEMORANDUM FOR (MAJCOM IA Office)

FROM: (Wing IA Office)

SUBJECT: Follow-up Number (#) to Information Assurance Assessment and Assistance Program (IAAP) visit, (include dates)

Section I

1. This is our second follow-up to the IAAP visit conducted by (MAJCOM IA Office) from (dates of assessment). The following deficiencies remain open from (initial report or follow-up number #), (date on initial reply or previous follow-up).

Section II

Item 1. (List section and question number)

a. Comments: (State the actions taken to correct the deficiency.)

b. Status: (State if Open or if can be recommended to closed.) (If the item is still open then provide the following) Estimated completion date is (provide a date).

2. (Additional comments.)

3. (List POC, office symbol, phone numbers, and e-mail address.)

Signature Block

1st Ind, (Unit commander)

MEMORANDUM FOR (MAJCOM IA Office)

(Provide a concurrence or nonconcurrence with corrective actions taken and definitive plans to resolve uncorrected deficiencies.)

Signature Block

Attachment 6

EXAMPLE OF ANNUAL SUMMARY REPORT

MEMORANDUM FOR (Address per **Table 3.**)

FROM: (Origination Office)

SUBJECT: Annual Summary Report of (Base or MAJCOM) for (year)

1. This annual summary is an assessment of (base or MAJCOM) of the following (units or bases): (Wing report, list all units assessed during that year. MAJCOM report, list all bases assessed during that year.)

Base/COMSEC Acct Number	**Date of assessment**	**Rating**
Lincoln AFB/CA 612345	3-8 Jun 03	Satisfactory

2. (Summarize all areas identified and corrective action that has been taken to correct them.)

COMSEC

a. (List the problem and fix action taken to resolve the problem.)

b. (List each item separately if there were problems in more than one area.)

COMPUSEC

a. (List the problem and fix action taken to resolve the problem.)

b. (List each item separately if there were problems in more than one area.)

(Include all sub-areas that apply: EMSEC, NCC, etc.)

3. (For MAJCOM report: identify all bases that are overdue for assessment and the reasons for noncompliance)

4. (List any additional comments)

5. (List POC, office symbol, phone numbers, and e-mail address.)

Signature Block